| | |
|---|---|
| Title | Commutation and Centralizers in Clone Theory (Algebras, Languages, Algorithms in Algebraic Systems and Computations) |
| Author(s) | Machida, Hajime |
| Citation | 数理解析研究所講究録 (2010), 1712: 101-110 |
| Issue Date | 2010-09 |
| URL | http://hdl.handle.net/2433/170231 |
| Right | |
| Type | Departmental Bulletin Paper |
| Textversion | publisher |

数理解析研究所講究録
第 1712 巻 2010 年 101-110



# Commutation and Centralizers in Clone Theory

Hajime Machida*

**Abstract**

Commutation theory is one of the central areas of research in universal algebra and clone theory. After giving the definitions of commutation, centralizers and endoprimal monoids, we present some of the results in this field which the author obtained during the past decade as the joint work with Ivo G. Rosenberg.

*Keywords:* clone; centralizer; endoprimal monoid

## 1 Introduction

What we need for constructing clone theory is simple and elementary: A fixed set $A$ and a set of (multi-variable) functions

$$f : A^n \longrightarrow A$$

defined on $A$. In universal algebra, an $n$-variable function on $A$ is called an operation on $A$ of arity $n$. We denote by $\mathcal{O}_A^{(n)}$ the set of all $n$-variable functions on $A$, i.e., $\mathcal{O}_A^{(n)} = A^{A^n}$. We also denote by $\mathcal{O}_A$ the set of all functions defined on $A$, i.e.,

$$\mathcal{O}_A = \bigcup_{n=1}^{\infty} \mathcal{O}_A^{(n)}.$$

For $1 \leq i \leq n$, the $i$-th *projection* $e_i^n$ of $n$ variables is defined by $e_i^n(x_1, \ldots, x_i, \ldots, x_n) = x_i$ for any $(x_1, \ldots, x_n) \in A^n$. $\mathcal{J}_A$ denotes the set of all projections $e_i^n$ $(1 \leq i \leq n)$ on $A$.

We consider (functional) composition among functions defined on $A$, and define a *clone* on $A$ as follows:

**Definition 1.1** *For a subset $C \subseteq \mathcal{O}_A$, $C$ is a* clone *if $C$ satisfies the following:*

(1) *$C$ is closed under (functional) composition.*

(2) *$C$ contains all the projections, i.e., $J_A \subseteq C$.*

**N.B.** In order to avoid confusion, we remark that our clone has no relation to biology !!

For a fixed set $A$, $\mathcal{L}_A$ denotes the set of all clones on $A$. It is known and easy to see that for any set$A$, $\mathcal{L}_A$ forms a lattice with respect to inclusion.

*(Until March 31, 2010) Mathematics Area, Hitotsubashi University, 2-1 Naka, Kunitachi, Tokyo 186-8601 Japan ⟨machida@math.hit-u.ac.jp⟩

In this paper, we let $A$ be a (non-empty) finite set $E_k$ where $E_k = \{0, 1, \ldots, k-1\}$ for $k > 1$. Then we write $\mathcal{O}_k^{(n)}$, $\mathcal{O}_k$, $\mathcal{J}_k$ and $\mathcal{L}_k$ instead of $\mathcal{O}_A^{(n)}$, $\mathcal{O}_A$, $\mathcal{J}_A$ and $\mathcal{L}_A$, respectively.

For the case where $k = 2$, that is, the case of Boolean functions, things are, in a sense, already settled.

**Theorem 1.1** *(E. Post)*
*The structure of $\mathcal{L}_2$ is completely determined. In particular, the cardinality of $\mathcal{L}_2$ is countable.*

On the other hand, the structure of $\mathcal{L}_k$ for each $k > 2$ is still largely unknown, remains mysterious and waits for further investigations. The following is one of few facts that we know up to now.

**Theorem 1.2** *(Janov and Muchnik)*
*For any $2 < k < \omega$ , $\mathcal{L}_k$ has the cardinality of the continuum.*

In this paper we focus our attention on commutation theory of clones. Commutation theory is one of the central areas of research in universal algebra and clone theory, which attracts many researchers in these fields. After giving the definitions of those terms such as centralizers and endoprimal monoids, we present some of the results that were obtained during the past decade as the joint work of the author with Ivo G. Rosenberg (Montréal). For most of the results presented here the proofs are omitted. (For the proofs refer to the references given at the end of this manuscript.)

# 2 Commutation

The main concept of this paper is **commutation** between two functions in $\mathcal{O}_A$.

**Definition 2.1** *For $f \in \mathcal{O}_k^{(m)}$ and $g \in \mathcal{O}_k^{(n)}$ we say that $f$* commutes *with $g$ (or, $f$ and $g$* commute*) if the following holds*

$$f(g(b_{11}, \ldots, b_{1n}), \ldots, g(b_{m1}, \ldots, b_{mn})) \quad = \quad g(f(b_{11}, \ldots, b_{m1}), \ldots, f(b_{1n}, \ldots, b_{mn}))$$

*for every $m \times n$ matrix $B = (b_{ij})$ over $E_k$.*

The definition may be better understood by the following picture.

$$\begin{array}{cccc|c}
b_{11} & b_{12} & \cdots & b_{1n} & g(\ldots, b_{1j}, \ldots) \\
b_{21} & b_{22} & \cdots & b_{2n} & g(\ldots, b_{2j}, \ldots) \\
\vdots & \vdots & & \vdots & \vdots \\
\vdots & \vdots & & \vdots & \vdots \\
b_{m1} & b_{m2} & \cdots & b_{mn} & g(\ldots, b_{m1}, \ldots) \\
\hline
f(\ldots, b_{i1}, \ldots) & f(\ldots, b_{i2}, \ldots) & \cdots & f(\ldots, b_{in}, \ldots) & f(g, \ldots) = g(f, \ldots)
\end{array}$$

We use the notation $f \perp g$ to mean that $f$ commutes with $g$. It is clear that $f \perp g$ is equivalent to $g \perp f$.

**Example**

(1) Let $f \in \mathcal{O}_k^{(1)}$ be any constant function and $g \in \mathcal{O}_k^{(n)}$ be any idempotent function. Then it is clear that $f$ and $g$ commute, i.e., $f \perp g$. Here, by definition, $g$ is *idempotent* if $g(x, \ldots, x) = x$ for

all $x \in E_k$.

(2) For $k = 3$ let $f,\, g \in \mathcal{O}_3^{(2)}$ be defined as follows:

$$f(x, y) = \begin{cases} 2 & \text{if } \ 2 \in \{x, y\} \\ 0 & \text{otherwise} \end{cases}$$

and

$$g(x, y) = \max\{x, y\}.$$

Then it is easily verified that $f$ and $g$ commute, i.e., $f \perp g$.

**Definition 2.2** *For $F \subseteq \mathcal{O}_k$ define*

$$F^* \quad = \quad \{\, g \in \mathcal{O}_k \mid g \perp f \ \text{ for all } \ f \in F \,\}$$

*$F^*$ is called the* centralizer *of $F$.*

**Lemma 2.1** *For any $F \subseteq \mathcal{O}_k$, the centralizer $F^*$ of $F$ is a clone.*

The following properties of centralizers are easy but important.

**Lemma 2.2** *For any $F,\ G \subseteq \mathcal{O}_k$ we have :*

(i) $F \subseteq F^{**}$

(ii) $F \subseteq G \implies F^* \supseteq G^*$

(iii) $F^{***} = F^*$

# 3 Centralizers of Monoids

For unary functions $f,\, g \in \mathcal{O}_A^{(1)}$ the composition $f \circ g$ is defined by setting

$$(f \circ g)(x) = f(g(x))$$

for all $x \in A$. The operation $\circ$ is associative and the identity function $s_1$ is the neutral element. Hence the algebra $\langle \mathcal{O}_A^{(1)};\, \circ,\, s_1\rangle$ is a *monoid.* A subset $M$ of $\mathcal{O}_A^{(1)}$ is a *submonoid* of $\mathcal{O}_A^{(1)}$ if $s_1 \in M$ and $M$ is closed under the operation $\circ$.

In this section, we determine centralizers of monoids of unary functions containing the symmetric group $S_k$ of $E_k$.

## 3.1 Results

Some years ago we posed the following problem.

**Problem**: For every $k \geq 3$, determine centralizers of all submonoids of $\mathcal{O}_k^{(1)}$ which contain the symmetric group $S_k$.

The complete solution to this problem was given in Machida and Rosenberg [MR 05]. It turned out that most of the centralizers of monoids containing the symmetric group are the same. This makes a clear contrast to the fact that, for any subgroups $G_1,\ G_2$ of $S_k$, $G_1^* \neq G_2^*$ whenever $G_1 \neq G_2$.

First we note a simple fact. Let $\mathcal{M}_k$ denote the set of submonoids of unary functions in $\mathcal{O}_k^{(1)}$.

**Lemma 3.1** *For any submonoid $M \in \mathcal{M}_k$,*

$$S_k \subset M \quad \Longrightarrow \quad S_k \cup \mathrm{CONST} \subseteq M$$

*Here,* CONST *denotes the set of all unary constant functions in $\mathcal{O}_k^{(1)}$.*

We present the results from smaller submonoids.

**Case 1**: $M = S_k$

For $n$-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n) \in E_k^n$ we say that $(x_1, \ldots, x_n)$ is *similar* to $(y_1, \ldots, y_n)$ if

$$x_i = x_j \iff y_i = y_j$$

for all $1 \le i, j \le n$.

**Proposition 3.2** *(Marczewski)*
*The centralizer $S_k^*$ of $S_k$ is the set of functions $f$ ($\in \mathcal{O}_k^{(n)}$) satisfying the following conditions.*

*(1) If $|\{x_1, \ldots, x_n\}| \neq k-1$ then*

*(i) $f(x_1, \ldots, x_n) = x_\ell$ for some $1 \le \ell \le n$ and*

*(ii) $f(y_1, \ldots, y_n) = y_\ell$ for $\forall\,(y_1, \ldots, y_n) \in (E_k)^n$ which is similar to $(x_1, \ldots, x_n)$.*

*(2) If $|\{x_1, \ldots, x_n\}| = k-1$ and $f(x_1, \ldots, x_n) = u$ for some $u \in E_k$ then*

*(i) $u = x_\ell$ for some $1 \le \ell \le n$ implies $f(y_1, \ldots, y_n) = y_\ell$ for $\forall\,(y_1, \ldots, y_n) \in (E_k)^n$ which is similar to $(x_1, \ldots, x_n)$ and*

*(ii) $u \in E_k \setminus \{x_1, \ldots, x_n\}$ implies $f(y_1, \ldots, y_n) = v$ where $v \in E_k \setminus \{y_1, \ldots, y_n\}$ for $\forall\,(y_1, \ldots, y_n) \in (E_k)^n$ which is similar to $(x_1, \ldots, x_n)$.*

**Case 2**: $M = S_k \cup \mathrm{CONST}$

**Proposition 3.3** *(1) For $k = 2$, the centralizer $(S_2 \cup \mathrm{CONST})^*$ is the clone*

$$\{\, f \in {S_2}^* \mid f : \text{idempotent} \,\}.$$

*(2) For every $k \ge 3$, the centralizer $(S_k \cup \mathrm{CONST})^*$ is the clone ${S_k}^*$.*

**Case 3**: $M \supset S_k \cup \mathrm{CONST}$

As an exceptional case for $k = 4$, we need to consider a submonoid which we call $M_2$.
For $u \in \mathcal{O}_k^{(1)}$ the *kernel* of $u$ is defined by

$$\ker u \;=\; \{(x, y) \in \boldsymbol{k}^2 \mid u(x) = u(y)\}.$$

Clearky, $\ker u$ is an equivalence relation on $E_k$. An equivalence class is called a block.

Let $k = 4$. We define $M_2$ as the submonoid consisting of $u \in \mathcal{O}_4^{(1)}$ satisfying one of the following conditions:

(i) $E_4 / \ker u$ has four singleton blocks, i.e., $u$ is a permutation on $E_4$.

(ii) $E_4 / \ker u$ has one block, i.e., $u$ is a constant function on $E_4$.

(iii) $E_4 / \ker u$ has two blocks of size 2, i.e., $u$ sends two elements in $E_4$ to an element in $E_4$ and the other two to another element in $E_4$.

Here, $E_4 \,/\, \ker u$ is the quotient set over $E_4$ induced by the equivalence relation $\ker u$. It is clear that $M_2 \supset S_4 \cup \mathrm{CONST}_4$.

**Proposition 3.4** *If $M \supset S_k \cup \mathrm{CONST}$ then the following holds.*

(i) *For $k = 3$ :* $\quad M^* = \mathcal{J}_3$

(ii) *For $k = 4$ :* $\quad$ *If $M \neq M_2$ then $M^* = \mathcal{J}_4$*

(iii) *For $k \geq 5$ :* $\quad M^* = \mathcal{J}_k$

**Note**: As mentioned below, the centralizer $M_2^*$ of $M_2$ for $k = 4$ is not equal to $\mathcal{J}_4$.

### 3.2 A Sufficient Condition for a Trivial Centralizer

We start with two properties of functions.

I. (Separation Property)
For all $a, b, c, d \in E_k$, if $\{a, b\} \neq \{c, d\}$ and $c \neq d$ then $M$ contains $f\,(= f_{cd}^{ab})$ which satisfies

$$f(a) = f(b) \quad \text{and} \quad f(c) \neq f(d).$$

II. (Fixed-Point-Free Property)
For every $i \in E_k$, $M$ contains $g_i$ which satisfies $g_i(i) \neq i$.

The following fact appears in Machida and Rosenberg [MR 04a] and [MR 04b].

**Lemma 3.5** *For any $M \in \mathcal{M}_k$, if $M$ satisfies the above conditions I and II then $M^* = \mathcal{J}_k$.*

It is an easy task to verify Proposition 3.4 from Lemma 3.5.

For the submonoid $M_2$ in the case $k = 4$, we can show that the centralizer of $M_2$ is not the least clone. Let the ternary function $m(x_1, x_2, x_3)$ $(\in \mathcal{O}_4^{(3)})$ be defined as follows:

$$m(x_1, x_2, x_3) = \begin{cases} x_1 & \text{if } \ x_1 = x_2 = x_3 \\ x_1 & \text{if } \ x_1 \neq x_2 = x_3 \\ x_2 & \text{if } \ x_2 \neq x_1 = x_3 \\ x_3 & \text{if } \ x_3 \neq x_1 = x_2 \\ y & \text{if } \ \{x_1, x_2, x_3, y\} \ = \ E_4 \end{cases}$$

It is readily verified that $m$ commutes with every member in $M_2$, i.e., $m \in M_2^*$. Hence, we have:

**Lemma 3.6** *$M_2^*$ is* not *the least clone $\mathcal{J}_4$.*

# 4 Kuznetsov Criterion

*Kuznetsov Criterion* was discovered by Kuznetsov in 1960's, and is an extremely useful tool ([Da 77]).

**Definition 4.1** *For $f \in \mathcal{O}_k^{(n)}$ and $\Sigma \subseteq \mathcal{O}_k$, $f$ is* parametrically expressible *(*p-expressible*) by $\Sigma$ if there exist $m \geq 1$, $\ell \geq 0$ and $g_i, h_i \in \mathcal{O}_k^{(n+\ell+1)}$ $(i = 1, \ldots, m)$ such that $g_i, h_i \in \langle \Sigma \rangle$ and*

$$\begin{aligned} f^{\square} \;=\; \{\, (x_1, \ldots, x_n, x_{n+1}) \mid \exists x_{n+2}, \ldots, x_{n+\ell+1} \in E_k,\ \forall i \in \{1, \ldots, m\}, \\ g_i(x_1, \ldots, x_{n+\ell+1}) \;=\; h_i(x_1, \ldots, x_{n+\ell+1}) \,\}. \end{aligned}$$

*Here, $f^{\square}$ means the graph of $f$, i.e., $f^{\square} = \{(x_1, \ldots, x_n, x_{n+1}) \mid f(x_1, \ldots, x_n) = x_{n+1}\}$*

Kuznetsov criterion states as follows:

**Theorem 4.1** *(Kuznetsov criterion)*
*For $f \in \mathcal{O}_k$ and $\Sigma \subseteq \mathcal{O}_k$, $f$ is p-expressible by $\Sigma$ if and only if $\Sigma^* \subseteq \{f\}^*$.*

Equivalently, it can be expressed as:

**Corollary 4.2** *(Kuznetsov criterion)*
*For $f \in \mathcal{O}_k$ and $\Sigma \subseteq \mathcal{O}_k$, $f$ is p-expressible by $\Sigma$ if and only if $f \in \Sigma^{**}$.*

**Example**. Let unary functions $j_0, j_1, s_3 \in \mathcal{O}_3^{(1)}$ be given below.

| | $j_0$ | $j_1$ | $s_3$ |
|---|---|---|---|
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 2 | 0 | 0 | 2 |

From $j_0$ and $j_1$ we get $s_3$ in the following sense:

$$s_3^{\square} = \{(x, y) \in (E_3)^2 \mid j_0(x) = j_1(y),\ j_1(x) = j_0(y)\ \}$$

Hence $s_3$ is p-expressible by $\{j_0, j_1\}$. Then, due to Kuznetsov Criterion, we have

$$s_3 \ \in \ \{\, j_0, j_1 \,\}^{**}$$

## 4.1 Centralizers of Subgroups of $S_k$

**Lemma 4.3** *For any subgroup $H$ of $S_k$ and any $s \in S_k$, $s$ is p-expressible by $H$ if and only if $s \in H$.*

**Proof** ($\Leftarrow$) Trivial.
($\Rightarrow$) Suppose that $s$ is p-expressible by $H$. Then, by definition, $s^{\square} = \{(x, y) \mid t(x) = u(y)\}$ for some $t, u \in H$. This is equivalent to $s^{\square} = \{(x, y) \mid (u^{-1}t)(x) = y\}$ for some $t, u \in H$, which implies that $s = u^{-1}t \in H$. □

**Theorem 4.4** *(Machida and Rosenberg)*
*The $*$-operator is injective over $S_k$, that is, for subgroups $H_1$ and $H_2$ of $S_k$,*

$$H_1^* = H_2^* \quad \Longrightarrow \quad H_1 = H_2.$$

**Proof** Suppose $H_1^* = H_2^*$ and $H_1 \neq H_2$. Then, w.l.o.g., we may take $s \in H_2 - H_1$. Now $H_1^* = H_2^*$ implies that

$$H_1^* \subseteq \{s\}^* (= \mathrm{Pol}\, s^{\square})$$

since $H_2^* = \bigcap_{t \in H_2} \mathrm{Pol}\, t^{\square}$. By Kuznetsov criterion, $s$ is p-expressible by $H_1$. Hence, by Lemma 4.3, we have $s \in H_1$. Contradiction. □

# 5 Endoprimal Monoids

In this section, we consider "endoprimal monoids", that is, the unary part of the centralizer of some set. Most of the results which will be presented in this section appeared in Machida and Rosenberg [MR 09] and [MR 10].

**Definition 5.1** *Let $\mathcal{A} = (A;\ F)$ be an algebra. For a map $\varphi : A \longrightarrow A$, $\varphi$ is an* endomorphism *of $\mathcal{A}$ if*

$$f(\varphi(x_1), \ldots, \varphi(x_n)) \quad = \quad \varphi(f(x_1, \ldots, x_n))$$

*holds for any $f \in F$ and all $(x_1, \ldots, x_n) \in A^n$.*

An endomorphism is naturally connected to commutation. Remember that for $f \in \mathcal{O}_k^{(1)}$ and $F \subseteq \mathcal{O}_k$, the fact that $f$ commutes with $F$, i.e., $f \perp F$, means that

$$g(f(x_1), \ldots, f(x_n)) \quad = \quad f(g(x_1, \ldots, x_n))$$

for any $g \in F$.

**Lemma 5.1** *For a map $\varphi : A \longrightarrow A$, the following are equivalent.*

(1) *$\varphi$ is an endomorphism of $\mathcal{A}$.*

(2) *$\varphi \perp F$, that is, $\varphi \perp f$ for all $f \in F$.*

(3) *$\varphi \in F^*$*

**Definition 5.2** *For a submonoid $M \subseteq \mathcal{O}_k^{(1)}$, $M$ is an* endoprimal monoid *if there exists $F \subseteq \mathcal{O}_k$ which satisfies $M = F^* \cap \mathcal{O}_k^{(1)}$.*

In other words, $M$ is an endoprimal monoid if $M$ is the unary part of a centralizer of some set $F \subseteq \mathcal{O}_k$.

**Lemma 5.2** *For a submonoid $M \subseteq \mathcal{O}_k^{(1)}$, $M$ is an endoprimal monoid if and only if $M = M^{**} \cap \mathcal{O}_k^{(1)}$.*

**Proof**
($\Leftarrow$) : Trivial.
($\Rightarrow$) : Suppose $M = F^* \cap \mathcal{O}_k^{(1)}$ for some $F \subseteq \mathcal{O}_k$. Then, since $M \subseteq F^*$, we have $M^{**} \subseteq F^{***} = F^*$. Taking the unary part, $M^{**} \cap \mathcal{O}_k^{(1)} \subseteq F^* \cap \mathcal{O}_k^{(1)} = M$. On the other hand, from $M \subseteq M^{**}$ it follows that $M = M \cap \mathcal{O}_k^{(1)} \subseteq M^{**} \cap \mathcal{O}_k^{(1)}$. Therefore, $M = M^{**} \cap \mathcal{O}_k^{(1)}$ as desired. □

For a submonoid $M \subseteq \mathcal{O}_k^{(1)}$ we sometimes write $M^+$ to mean $M^+ = M^{**} \cap \mathcal{O}_k^{(1)}$.

**Lemma 5.3** *For a submonoid $M \subseteq \mathcal{O}_k^{(1)}$, $M^+$ satisfies the following properties.*

(1) *$M^+$ is an endoprimal monoid.*

(2) *$M \subseteq M^+$*

(3) *$M^+$ is the largest submonoid consisting of "endomorphisms" of the algebra $\langle E_k\ ;\ M \rangle$*

Up to now, not many examples of endoprimal monoids are known. In the sequel, we shall mostly concentrate on the ternary case, that is, the case where the base set is $E_3 = \{0, 1, 2\}$.

| | $j_0$ | $j_1$ | $j_2$ | $j_3$ | $j_4$ | $j_5$ | $u_0$ | $u_1$ | $u_2$ | $u_3$ | $u_4$ | $u_5$ | $v_0$ | $v_1$ | $v_2$ | $v_3$ | $v_4$ | $v_5$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 1 | 1 | 2 | 2 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 2 | 0 | 2 | 0 | 2 | 1 | 2 | 1 | 2 | 1 | 2 |
| 2 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 2 | 0 | 2 | 2 | 1 | 1 | 2 | 1 | 2 | 2 |

| | $c_0$ | $c_1$ | $c_2$ |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 1 | 2 |

| | $s_1$ | $s_2$ | $s_3$ | $s_4$ | $s_5$ | $s_6$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 2 | 2 |
| 1 | 1 | 2 | 0 | 2 | 0 | 1 |
| 2 | 2 | 1 | 2 | 0 | 1 | 0 |

Table 1: Unary Functions in $\mathcal{O}_3^{(1)}$

## 5.1 Unary Functions and Submonoids on $\{0, 1, 2\}$

As is well-known, the number of unary functions over $E_3$ is 27. They are shown in Table 1. Much less known is the number of submonoids of unary functions over $E_3$. Due to D. Lau ([La 84], [La 06]), the number of submonoids of unary functions over $E_3$ is 700.

Let us search for an endoprimal monoid containing both $j_0$ and $j_1$. Repeated applications of "Kuznetsov Criterion" imply the following. (We omit the details here.)

**Lemma 5.4** *If* $M\,(\subseteq \mathcal{O}_3^{(1)})$ *is an endoprimal monoid and* $\{\, j_0,\, j_1 \,\} \in M$ *then*

$$P_2 \subseteq M \;\; (= M^+)$$

*where* $P_2 = \{c_0, c_1, c_2\} \cup \{\, j_0, j_1, j_4, j_5\} \cup \{\, u_0, u_1, u_4, u_5\} \cup \{\, v_0, v_1, v_4, v_5\} \cup \{\, s_1, s_3\}$.

Actually, $P_2$ is the submonoid #1227 in Lau's list. At this point, we do not know if $P_2$ is endoprimal or not. The following "witness lemma" will tell us that, in fact, $P_2$ is endoprimal.

## 5.2 Witness Lemma

The following lemma wa given in Machida and Rosenberg [MR 10].

**Lemma 5.5** *(Witness Lemma)*
*For a submonoid* $M \subseteq \mathcal{O}^{(1)}$ *of unary functions and a subset* $S \subseteq \mathcal{O}$, *suppose the following conditions (i) and (ii) hold:*

(i) *For any* $f \in M$ *and any* $u \in S$ *it holds that* $f \perp u$.

(ii) *For any* $g \in \mathcal{O}^{(1)} \setminus M$ *there exists* $w \in S$ *such that* $g \not\perp w$.

*Then* $M$ *is endoprimal.*

**Definition 5.3** *S in the lemma will be called a* witness *for an endoprimal monoid* $M$.

The proof is straightforward, but, for the reader's sake, we give it below.

**Proof of Lemma** Condition (i) implies $S \subseteq M^*$, from which it follows that $M^{**} \subseteq S^*$. Condition (ii) asserts that, for all $g \in (\mathcal{O}^{(1)} \setminus M)$, it holds that $g \notin S^*$. Then it follows that, for all $g \in (\mathcal{O}^{(1)} \setminus M)$, $g \notin M^{**}$, because we have $M^{**} \subseteq S^*$ as stated above. Hence $(\mathcal{O}^{(1)} \setminus M) \cap M^{**} = \emptyset$.
On the other hand, $M \subseteq M^{**}$, in general. Therefore $M = M^{**} \cap \mathcal{O}^{(1)}$, i.e., $M = M^+$. □

**Corollary 5.6** *(Special Case where $S$ is a singleton)*
*For a submonoid $M \subseteq \mathcal{O}^{(1)}$ of unary functions and a function $f \in \mathcal{O}$, if $f \perp M$ and $f \not\perp (\mathcal{O}^{(1)} \backslash M)$ then $M$ is endoprimal.*

## 5.3 Some Endoprimal Monoids on $\{0, 1, 2\}$

We show two applications of the witness lemma.

### 5.3.1 Application of Witness Lemma (1)

Let $m \in \mathcal{O}_3^{(3)}$ be a witness, which is defined as follows:

$$m(x,y,z) = \begin{cases} x & \text{if} \quad x = y \ \text{or} \ x = z \\ y & \text{if} \quad y = z \\ 2 & \text{if} \quad \{x,y,z\} = \{0,1,2\} \end{cases}$$

In other words, $m$ is the majority and totally symmetric function satisfying the following.

(i) $\quad m(a,a,b) = a \quad$ for all $a, b \in E_3$

(ii) $\quad m(0,1,2) = 2$

Then it is easily verified that (1) the function $m$ commutes with all functions in $P_2$, i.e., $m \in P_2{}^*$ and (2) $m$ does not commute with any function in $\mathcal{O}_3^{(1)} \backslash P_2$. Therefore, the witness lemma implies:

**Proposition 5.7** *$P_2$ is an endoprimal monoid.*

Moreover, we note that $P_2$ is shown to be a maximal endoprimal monoid.

### 5.3.2 Application of Witness Lemma (2)

For each subset $S$ of unary functions, i.e., $S \subseteq \mathcal{O}_3^{(1)}$, one can construct an endoprimal monoid which has $S$ as its witness.

**Example 1**. For $c_0 \in \mathcal{O}_3^{(1)}$ take $S = \{c_0\}$ as a (singleton) witness. It is easy to check that the set of unary functions which commute with $c_0$ is $\{c_0, j_1, j_2, j_5, u_1, u_2, u_5, s_1, s_2\}$. Hence, by the witness lemma, we see that

$$M(c_0) = \{ c_0, j_1, j_2, j_5, u_1, u_2, u_5, s_1, s_2 \}$$

is an endoprimal monoid.

**Example 2**. Let $S = \{c_0, j_1\}$ be a doubleton consisting of $c_0$ and $j_1 \in \mathcal{O}_3^{(1)}$. It is readily verified that the set of unary functions which commute with $j_1$ is $\{c_0, c_1, j_1, j_4, u_2, s_1\}$. Together with the result given in Example 1, we see that the set of unary functions which commute with both $c_0$ and $j_1$ is $\{c_0, j_1, u_2, s_1\}$. Hence, by the witness lemma, it follows that

$$M(c_0, j_1) = \{ c_0, j_1, u_2, s_1 \}$$

is an endoprimal monoid.

We have the complete list of the endoprimal monoids having subsets ($\subseteq \mathcal{O}_3^{(1)}$) of unary functions as their witnesses. Below we give the summary of this list. For more precise description the reader is referred to [MR 10].

**Proposition 5.8** *Over $E_3$, there are* 51 *endoprimal monoids each having a subset of $\mathcal{O}_3^{(1)}$ as its witness.*

(1) *(Singleton witnesses) Out of 27 unary functions $f$ in $\mathcal{O}_3^{(1)}$, there are 26 different endoprimal monoids $M(f)$ each having singleton witness $\{f\}$. An exception is for $s_4$ and $s_5$, where we have $M(s_4) = M(s_5)$.*

(2) *(Doubleton witnesses) There are 25 endoprimal monoids which have doubleton witnesses (and have no singleton witnesses).*

(3) *(Larger witnesses) There is no endoprimal monoid over $E_3$ which requires a witness, consisting of unary functions, whose size is greater than* 2.

## References


[Da 77] Danil'tchenko, A. F., Parametric expressibility of functions of three-valued logic (in Russian), *Algebra i Logika*, **16**, 1977, 397-416; English traslation: *Algebra and Logic*, **16**, 1977, 266-280.

[Da 79] Danil'tchenko, A. F., On parametrical expressibility of the functions of $k$-valued logic, *Colloquia Mathematica Societatis János Bolyai*, **28**, Finite Algebra and Multiple-Valued Logic, 1979, 147-159.

[HMR 06] Haddad, L., Machida, H. and Rosenberg, I. G., Theoretical basis of commutation theory for partial clones, *Proceedings 36th International Symposium on Multiple-Valued Logic*, IEEE, 2006, p.22:1-6 (DVD).

[La 84] Lau, D., Die Unterhalbgruppen von $(P_3^1; *)$, *Rostock Math. Colloq.*, **26**, 1984, 55-62.

[La 06] Lau, D., Function Algebras on Finite Sets, *Springer Monographs in Mathematics*, Springer, 2006.

[MMR 02] Machida, H., Miyakawa, M. and Rosenberg, I. G., Some results on the centralizers of monoids in clone theory, *Proc. 32nd Int. Symp. Multiple-Valued Logic*, IEEE, 2002, 10-16.

[MR 03] Machida, H. and Rosenberg, I. G., On the centralizers of monoids in clone theory, *Proc. 33rd Int. Symp. Multiple-Valued Logic*, IEEE, 2003, 303-308.

[MR 04a] Machida, H. and Rosenberg, I. G., Monoids whose centralizer is the least clone, *Proc. 34th Int. Symp. Multiple-Valued Logic*, IEEE, 2004, 102-108.

[MR 04b] Machida, H. and Rosenberg, I. G., On centralizers of monoids, *Novi Sad Journal of Mathematics*, Vol. **34**, No. **2**, 2004, 153-166.

[MR 05] Machida, H. and Rosenberg, I. G., Centralizers of monoids containing the symmetric group, *Proceedings 35th International Symposium on Multiple-Valued Logic*, IEEE, 2005, 227-233.

[MR 09] Machida, H. and Rosenberg, I. G., On endoprimal monoids in clone theory, *Proc. 39th Int. Symp. Multiple-Valued Logic*, IEEE, 2009, 167-172.

[MR 10] Machida, H. and Rosenberg, I. G., Endoprimal monoids and witness lemma in clone theory, to appear in *Proceedings 40th International Symposium on Multiple-Valued Logic*, IEEE, 2010.